What is claimed is:

1. A security container that secures a document component by encapsulating, within the security container, the document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component.

2. The security container according to Claim 1, wherein the security container secures a portion of a higher-level document.

3. The security container according to Claim 2, wherein the higher-level document has more than one portion secured by security containers.

4. A method of securing document content using security containers, comprising the step of encapsulating, within a security container, a document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component.

5. The method according to Claim 4, wherein the key distribution information further comprises an identification of one or more users and/or processes that are authorized to access the document component.

6. The method according to Claim 5, wherein the key distribution information further

comprises a symmetric key that encrypted both the document component and the conditional logic that are encapsulated within the security container, wherein the symmetric key is stored in an encrypted form for decryption by the authorized users and/or processes.

7. The method according to Claim 6, wherein the encrypted form of the symmetric key comprises a separate version of the key for each distinct user, process, group of users, or group of processes, wherein the separate version has been encrypted with a public key associated with the corresponding distinct user, process, group of users, or group of processes.

8. The method according to Claim 5, wherein the authorized users and/or the authorized processes are specified individually or as groups.

9. The method according to Claim 4, wherein the conditional logic further controls access to the document component.

10. The method according to Claim 9, wherein the key distribution information further controls access to the conditional logic.

11. The method according to Claim 4, wherein the document component and the conditional logic are encrypted before encapsulation within the security container.

12. The method according to Claim 4, wherein the security container is encoded in structured

document format.

13. The method according to Claim 12, wherein the structured document format is Extensible Markup Language ("XML") format.

14. The method according to Claim 5, wherein the identification of the one or more users and/or processes comprises an identification of at least one group, the group having as members one or more of the users and/or processes.

15. The method according to Claim 14, wherein the members are determined dynamically, upon receiving a request to access to the document component.

16. The method according to Claim 15, wherein the dynamic determination further comprises accessing a repository where the members of the group are identified.

17. The method according to Claim 4, further comprising the steps of:

receiving, from a requester, a request to access the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and rejecting the request when the programmatically determining step has a negative result.

18. The method according to Claim 17, wherein the conditional logic evaluates at least one of: an identity of the requester; a device used by the requester; a context of the requester; a zone of an application used by the requester; a user profile of the requester; and a target destination of the request.

19. A computer program product for securing document content using security containers, the computer program product embodied on one or more computer-readable media and comprising:

computer-readable program code means for receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

computer-readable program code means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

computer-readable program code means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the computer-readable program code means for programmatically determining yields a positive result, and for rejecting the request when operation of the computer-readable program code means for programmatically determining yields a negative result.

20. A system for securing document content using security containers, comprising:

a security container that encapsulates a document component, conditional logic for controlling operations on the document component, and key distribution information usable for controlling access to the document component;

means for receiving, from a requester, a request to access the document component;

means for programmatically determining, using the key distribution information, whether the requester is authorized to access the document component; and

means for programmatically evaluating, using the conditional logic, whether the request can be granted, when operation of the means for programmatically determining yields a positive result, and for rejecting the request when operation of the means for programmatically determining yields a negative result.

21. The system according to Claim 20, wherein the security container is embedded within a document.

22. The system according to Claim 20, wherein the security container encapsulates the document component on a system clipboard.

23. The system according to Claim 20, wherein the security container is placed on a user interface.

24. The system according to Claim 20, wherein the security container encapsulates the

document component for exchange using interprocess communications.

25. The system according to Claim 20, wherein the security container encapsulates the document component for exchange using a messaging system.

26. The system according to Claim 20, further comprising means for copying the document component to a target destination, wherein the means for copying copies the entire security container in order to copy the document component.

27. A method of securing document content using security containers, comprising steps of:

receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component;

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and for rejecting the request when the programmatically determining step has a negative result; and

charging a fee for carrying out one of more of the receiving, programmatically determining, and programmatically evaluating steps.

28. A method of securing document content using security containers, comprising steps of:

receiving, from a requester, a request to access document content, wherein the document content is encapsulated as a document component within a security container along with conditional logic for controlling operations on the document component and key distribution information usable for controlling access to the document component;

programmatically determining, using the key distribution information, whether the requester is authorized to access the document component;

programmatically evaluating, using the conditional logic, whether the request can be granted, when the programmatically determining step has a positive result, and for rejecting the request when the programmatically determining step has a negative result; and

charging a fee to the requester when the programmatically evaluating step determines that the request can be granted.